DIGITAL FINANCIAL FRAUDS: A CRITICAL ANALYSIS OF THE CYBER LAWS IN INDIA

SHORT SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

by

Manisha Ambawta
Registration No. MRULWDM012K230066

Under the supervision of

Dr. Aditi Choudhary
Assistant Professor, Manav Rachna University

Department of Law
School of Law

MANAV RACHNA, UNIVERSITY
Sector-43, Aravali Hills, Faridabad

Year *2025*

MANAV RACHNA UNIVERSITY

MANAV RACHNA UNIVERSITY
Sector-43, Aravali Hills, Faridabad

Date 4/4/25

DECLARATION BY THE SCHOLAR

I hereby declare that the short synopsis **"Digital Financial Frauds: A Critical Analysis Of The Cyber Laws In India"** being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in the Department of Law under the School of Law of Manav Rachna University, Faridabad during the academic year 2024-25.

It is bonafide record of original work carried out under the supervision of **Dr. Aditi Choudhary** and has not been submitted in full or part to any other university or institute for degree or diploma.

Manisha Ambawta
MRULWDM012K230066

PDF Scanner ACE Scanner

ii

MANAV RACHNA UNIVERSITY

MANAV RACHNA UNIVERSITY
Sector-43, Aravali Hills, Faridabad

Date 4/4/25

CERTIFICATE BY SUPERVISOR

This is to certify that, the short synopsis entitled **"Digital Financial Frauds: A Critical Analysis Of The Cyber Laws In India"** is an original piece of work done by research scholar **Manisha Ambawta** under the supervision of **Dr.Aditi Choudhary** for the degree of Doctor of Philosophy in the Department of Law under the School of Law of Manav Rachna University, Faridabad during the academic year 2024-25

Further, it is certified that the short synopsis is within the plagiarism limit and copy of the same is attached as per the University norms.

Supervisor
Dr. Aditi Choudhary
Assistant Professor

ABSTRACT

With most transactions going digital in India at such a rapid pace, there is a rise in digital financial frauds posing a great challenge for individuals and businesses and financial institutions as well. Even though the Indian government has introduced several cyber laws, including the Information Technology Act, 2000, and regulatory frameworks by the Reserve Bank of India, the increasing sophistication of cybercriminals continues to expose gaps in the current legal and enforcement frameworks. In this study, we critically evaluate the Indian cyber laws related to digital financial fraud, identify the legal vacuum and recommend measures to strengthen the cyber security architecture. Research Objectives: To devise innovative technologic solutions for security enhancement of online banking system To analyze efficacy of India's legal framework to prevent, detect and prosecute online financial fraud Exploration of cyber security strategies to combat malicious activities Analyzing the judicial interpretation and application cyber laws in reference to digital financial crimes, including review of recent case laws and court rulings Comparison of India's cyber laws with International best practices to identify areas of improvement. Through an analysis of legal formats, case studies, and upcoming cyber-attacks, this paper evaluates the effectiveness of India's cyber security legislation. Through an understanding of enforcement gaps, jurisdictional limitations, and the evolving cyber threat landscape, this research seeks to provide pragmatic recommendations to strengthen India's legal and technological capabilities against financial fraud. Through this, the findings aim to support a more secure digital financial ecosystem by calling for critical reforms that help mitigate the risks of cyber fraud within India's financial sector.

Keywords: Digital Financial Fraud, Cyber security Laws, Information Technology Act, Financial Institutions and Cybercriminals

S. No	Table of content	P. No
1	Introduction	1-3
1.1	Background of the Study	3-4
1.2	Statement of the Problem	4-5
1.3	Research Gap	5
1.4	Case Laws	5-7
2	Literature Review	8-13
3	Research Objective	14
4	Research Methodology	14
5	Hypothesis	15
6	Research Questions	15
7	Tentative Chapterization	16
8	Bibliography	17-19

1. INTRODUCTION:

Advancements in e-commerce technology: The nature of e-commerce has been transformed by its considerable digital technology. As one of the fastest-growing digital economies, India has seen exponential growth in digital financial services — online banking, e-wallets, Unified Payments Interface (UPI) and crypto currency transactions. But this digital know-how also comes with an alarming rise in financial frauds, making the need for cyber security and legal fabric ever more vital (Kumar, Vijay 2023). With economic transactions shifting onto the internet, cybercriminals have developed complex ways to take benefits of their computer systems' weaknesses, resulting in unrestricted access, identity fraud, phishing, online cons, and monetary data breaches. As a result, the significance of cyber laws in India has grown tenfold to protect individuals and organizations from these growing threats.

Digital financial frauds cover a wide range of illegal acts, such as hacking, phishing, vishing, card skimming, malware attacks, digital payment frauds, etc. Beju, et, al. (2023). The finance sector, in particular is under siege, with cybercriminals using artificial intelligence, deepfake manipulation and ransomware against financial institutions and unwitting Members of the Public. Therefore, there is an increased requirement for a more dynamic and effective judicial legal structure to supplement the rise of instant cyber scams predominant in the Indian Region in order to preserve the security of monetary transactions. Delimitations of the Indian Legal Framework Regulating Cybercrime and Corresponding Digital Financial Fraud Conclusion Jaiswal, et, al. (2022): Despite being deliberately established to fight against digital financial frauds, the legal infrastructure of the nation still holds many loopholes and thus makes it highly probable for cybercriminals to carry out their schemes against innocent victims of irregularities.

The law applicable to the digital financial frauds in India is primarily based on the provisions of the Information Technology Act, 2000 (amended in 2008), Indian Penal Code (IPC), Reserve Bank of India (RBI) and various sectoral laws. The IT Act: Basics The IT Act is considered the primary law, providing the entire structure of cyber law in India, regulating electronic transactions, cyber offences, and digital security Kashyap, et, al. (2023). Furthermore, offences under sections involving fraud, cheating and forgery

which are aspects prevalent in a digital financial ecosystem fall within the ambit of the IPC. However, cybercriminals often take advantage of regulations' holes, jurisdiction concerns, and enforcement challenges, consequently leading to financial fraud prevention being a complex and ever-changing job.

Users, however, find themselves at risk due to their lack of education around these tools. And, as cybercriminals look to prey on unsuspecting individuals who have little idea of how to keep themselves protected online, phishing, identity theft, and social engineering frauds are all on the rise. In fact, the current state of user security on the internet is so poor because most financial transactions do not have strong authentication mechanisms. Though security mechanisms such as two-factor authentication, secure banking practices, and transaction monitoring have been incorporated by regulatory institutions like the RBI, cybercriminals continue to devise methodologies of smuggling through the glue. So the dissection of our legal framework that balances equality with justice is evermore critical. The silent but deadly parallel: Cross-border cybercrimes as financial transactions become more global in nature, it is also possible that cyber criminals operating from different jurisdictions can target Indian financial systems, complicating law enforcement efforts, Qian, Xu. (2024). Lack of mechanisms for international legal cooperation also only makes it more difficult to prosecute and extradite cybercriminals. India has signed pacts with international organisations on tackling cybercrime, enforcement of cyber law at the international level remains one of the biggest challenges due to legal differences across countries.

The rise of crypto currencies and decentralized financial systems poses another challenge for Indian regulators. Crypto currencies, since they are anonymous and decentralized, are one the most preferred medium for financial frauds and money laundering as well as illegal transaction. Although India has introduced cryptocurrency trading and transaction regulations, the lack of clarity surrounding their legal status has hindered action against fraudulent schemes from being taken effectively Kumar, et, al. (2023) While the Reserve Bank of India along with the central government has suggested strict regulations, the natures of digital assets keep changing as per the demand and hence policy needs to evolve constantly along with legal measures.

Additionally, the responsibility of financial bodies toward deflecting digital financial frauds must not be ignored. It is the bank, payment service providers, and fintech

companies that are on the front line of implementation of cyber security measures to prevent fraud against consumers. Mitigating Financial Risks: The buyers are required to address financial risks such as to comply with regulations, implement fraud detection mechanisms, and create secure payment gateways Khurana, et. Al. (2020). As shown in, despite improvements in fraud detection technology, incidents of data theft and fraudulent transactions persist, emphasizing the continuing necessity of significant legal safeguards and improvements in cyber security protocols. The increasing digital economy in India is greatly challenged by digital financial frauds. Though existing laws and regulatory frameworks address some level of protection, gaps in legal enforcement, technological vulnerability, and consumer unawareness still keep financial fraud alive. Stronger cyber laws, improving digital literacy, international cooperation, and enhanced cyber security are critical to combating the growing menace of digital financial frauds, Juneja, et. al. (2024). The objective of this study is to critically evaluate the existing cyber laws in India and the loopholes in their application, and to provide suggestions to strengthen the legal basis of protection for digital finance in the Indian territory.

1.1 Background of the Study

The government initiatives of Digital India, demonetization, and promotion of cashless payments have also accelerated this transition, leading to the rise of digital financial transactions in India Fouillet, et. al. (2021). As more people embrace digital financial services, cybercriminals have discovered new ways of exploiting vulnerabilities in digital payment systems. Such online financial frauds, including phishing attacks, unauthorized transactions, and data breaches, have increased the need for stronger legal frameworks and regulatory mechanisms to ensure digital financial security. In India, the principal law dealing with cybercrimes is the Information Technology Act, 2000. The laws governing these must accordingly be amended and updated as such frauds are continuously evolving where they are being committed from different mediums and faces a different challenge in the sense that the perpetrators are often tech-savvy betterment than the actual enforcement agencies. However, enforcement continues to pose a challenge, despite the guidelines that the Reserve Bank of India (RBI) has been responsible for instituting that provide greater clarity on measures that financial institutions can take to bolster cyber security Ratnoo, et, al. (2024).

Additionally, the absence of digital knowledge among users has led to an increase in financial frauds, with stems of social engineering fraud and scam schemes leading such

individuals to become victims. The rising adoption of crypto currencies has also complicated the legal framework as regulators defer between innovation and payment security in the financial ecosystem. This study seeks to critically review the cyber laws and assesses the legal framework involved in-ment currency/financial frauds in India, with the aim to highlight significant legal gaps, enforcement problems, and policy needs. The study is anticipated to enhance a safer and secure digital financial ecosystem by evaluating the applicability of current laws and proposing recommendations.

1.2 Statement of the Problem

With the growing number of digital financial transactions in India, cyber frauds have also increased in recent years, impacting individuals, enterprises, and finance institutions. Thus, while there are cyber laws in place and regulatory frameworks implemented by the Reserve Bank of India for the conduct of digital transactions, the number of digital financial frauds is increasing, exposing the loopholes in the existing legal and enforcement structure. The evolution of cybercriminal and the poor awareness of cyber laws, cyber security and digital literate to the people are adding to the challenge, on the other side the cyber laws in India is getting old in today's environment, old and obsolete cyber laws can't protect country and India must to reconsider and to reinforce them. One of the challenges of digital financial fraud is that existing legal content cannot keep up with rapidly changing cyber threats. Current cyber laws are mostly generic and fail to mention newer fraud techniques, like deepfake fraud, AI based phishing and frauds by means of crypto currency. Because Cybercriminals crossing more jurisdictional lines poses a jurisdictional challenge to the prosecution and extradition of the assailants and thus brings them in a little deeper towards prosecution and extradition below foreign territory.

The fact is that cyber laws are often not enforced EFG, Ajayi (2015). Although the legal framework establishes the foundation for financial stability and fraud deterrence, deficient enforcement and slow judicial responsiveness have enabled cybercriminals to leverage aspects of regulations without adequate deterrents Ajayi, et, al. (2016). In general, this is making it challenging to track and prosecute digital fraudsters which in turn leads to a looming increase in online scams, resulting in financial losses and eroding trust in digital financial platforms. In addition, the digital divide and lack of awareness among users make the situation worse. Most of them, specifically those hailing from rural

and financially weaker sections, are not aware about secured online transactional practices, which puts them at risk of economic frauds. The motivation behind this study is to examine these issues and suggest legal, policy and technological reforms that would strengthen the overall cyber security architecture of India to combat digital financial frauds effectively.

1.3 Research Gap

Although these above laws and provisions exist in India, there are gaps in a comprehensive understanding of what constitutes digital financial fraud Saluja, et. al. (2024). However, existing studies have mainly examined the nature of cyber laws itself and many of them have not critically analyzed their potential of combating the newly introduced financial fraud methods like AI phishing, deep fake scams, and hyper currency. Moreover, cyber threats are constantly evolving, and legal provisions need to be continuously revised to meet the new challenges, which have not been sufficiently addressed in the current body of literature. The enforcement of cyber laws is a second research gap. The legislative measures offer a framework, but without empirical studies on enforcement procedures, judicial responses, and case studies, their functional implications are largely unknown Collier, et, al. (2022). Also, it also creates challenges for law enforcement agencies as cybercriminals often operate outside national borders, making cross-border financial frauds an area that needs further research. This paper seeks to address these lacunae, through a critical examination of existing cyber laws, an assessment of the implementation challenges as well as a prescriptive, recommendations-based discussion on relevant legal and other reforms needed relevant to Indian digital financial system.

1.4 Case Laws:

The UPI Fraud at Yes Bank (2023)

Fraudsters used the Unified Payments Interface (UPI) to steal money from customers' Yes Bank-affiliated accounts in a well-known case. Victims were tricked into sharing their UPI PINs over fake customer support calls in a social engineering scam. While victims of the fraud did report to the Cybercrime Reporting Portal, they had frequently failed to do so in time and suffered irreversible financial losses. Judicial Interpretation: Banks were held to the standards of rigorous security practices. Despite this, courts focused on

consumer education and the obligations of banks under the RBI's "zero liability" regime — for fraud victims reporting the same to the police in a timely manner.

In 2023, **the Bombay High Court, in the case of Jaiprakash Kulkarni v. Banking Ombudsman & Bank of Baroda**, directed the bank to reimburse unlawful transactions as the bank failed to stop the addition of fraudulent beneficiary. The court upheld banks' liability in cyber fraud cases and denounced the disregard for RBI guidelines.

State of Tamil Nadu v. Prabhakaran (2022): The Madras High Court ordered law enforcement to speed up investigations into digital financial fraud and stressed the importance of victims reporting phishing scams as soon as possible.

Shreya Singhal vs. Union of India (2015) Because Section 66A infringed upon the right to freedom of speech and expression, the Supreme Court declared it unconstitutional. By defining the parameters of what qualifies as an online offense, this ruling affected the prosecution of cybercrimes, including financial frauds. The case brought attention to the need for India's cyber laws, particularly those pertaining to digital financial frauds, to be more specific and focused.

PNB Fraud Case (Punjab National Bank Scam) 2018 One of the biggest banks in India, Punjab National Bank, discovered a significant financial scam in 2018 that involved the use of phony Letters of Undertaking (LoUs) given to businesses owned by Mehul Choksi and Nirav Modi. The scam, which involved unauthorized transactions through SWIFT (Society for Worldwide Interbank Financial Telecommunication), totaled more than rs. 11,000 crores. This case also highlighted issues around cyber law enforcement challenges, regulatory supervision, and greater scrutiny of financial systems.

Digital payment fraud in 2024 saw a fivefold increase in the number of reported fraud cases compared to 2020, according to the Reserve Bank of India, mainly due to the sharp increase in UPI transactions. Due to this surge and the magnitude of financial losses associated with it, consumer protection has become a top priority for the RBI, and it has initiated measures to enhance the security of digital transactions. Allegations from Indian Cyber Crime Coordination Center (I4C): Over 740 thousand complaints in January-April 2024 Most of which were financial fraud

Given the sophistication of financial scams, this increase emphasizes the need for improved security measures and stricter enforcement to protect users. The existing cyber

laws in India, although fundamental, fall short in effectively tackling the intricacies and swift developments of digital financial frauds. These new techniques, which include but are not limited to the applications of technology such as AI, machine learning, and block chain, are exposing serious gaps in both the law as enacted and the enforcement mechanisms in place. India has made some meaningful strides in its cyber-law framework. This study notes that these laws have not kept pace with modern technology or global practices, and places a risk on financial institutions and consumers.

2. LITERATURE REVIEW

The subject of digital financial frauds and the related legal frameworks have been widely discussed in the literature over the past years due to the pressing need to combat these types of cybercrimes in the digital economy. The purpose of this review is to synthesize existing research and reports on the subject under consideration within the Indian context while touching upon the global perspectives for Harnessing Cyber Threats into Insights CYBER PRAVAHA, Fifth Quarterly Issue, Government of India Ministry of Home Affairs, 1st April - 30th June 2022 I4C strives to enhance the capacity of Law Enforcement Agencies (LEAs) or improve coordination between the various stakeholders and LEAs. Cyber Crime Awareness– Awareness in preventing cyber crime among public has been one of the pivotal emphasis initiated by I4C under NCEMU. I4C has also been helping States/UTs in training Police Officers and Judicial Officers in the field of cyber forensics, cyber hygiene, cyber-criminology, etc.

Guanglin Sun a b,Ting Li, et. Al, (2023) Digital finance and corporate financial fraud, International Review of Financial Analysis, Volume 87, May 2023 The conclusionDAFC set low access barriers by implementing money-lending models based on unique companies and group of people. Corporate financial fraud harms the interests of investors and endangers the sound development of zthe capital market. As for the theory, Corporate finance fraud has an essential significant theory value, and in practical; there has been relatively fast development in the digital finance in recent years and how to find out the digital finance to fight the corporate financial fraud is still the hot field which researchers are considering. Using empirical data of economic indicators to investigate the direct effect, inherent mechanism and heterogeneous effect of digital financial development on corporate financial fraud, based on a sample of A-share listed firms in China from 2011 to 2020. The findings suggest that digital finance could greatly curtail corporate financial fraud. Findings: The effects and extensive penetration of digital finance have been shown to effectively discourages corporate financial fraud in the study.

Cybercriminal behavior and punishment deterring from law enforcement and social prevention also is evolving (Brent Clyton Harker 2017). The age of cyber crime can be divided into four stages, the germination stage, the rapid development stage, the broad development stage and the reuse stage. In addition, the cyber crime related criminal-law reform was never fully in synch with Research Gaps Identify.

David Broadstock, Corporate site visits, private monitoring and fraud: Evidence from China, Finance Research Letters Volume 40, May 2021, 101780 Corporate site visits (CSVs) create an in-person channel for outsiders to meet with corporate managers. In addition to collecting information from managers via such visits, investors have the opportunityto provide external knowledge and/or personal recommendations to managers. We submit in this study that corporate and managerial fraud is discouraged by means of private monitoring through CSVs. We exploit Chinese data from 2009-2018 to empirically examine, and demonstrate a strongly negative relation between how often a corporate site visit occurs and both the fate and the probability of firm fraud and manager fraud. This result holds for alternative measurements for CSVs, and potential endogeneity issues. In addition, we demonstrate that the impact of CSVs is weaker for well-governed firms

Waleed Hilal Financial Fraud: An Overview of Techniques for Anomaly Detection and Recent Developments, Expert Systems with Applications Volume 193, 1 May 2022, 116429. These include credit card fraud, healthcare and automobile insurance fraud, money laundering, fraud and insider stock trading. Fraud prevention systems, on the other hand, do not offer sufficient protection against such criminal offenses However, supervised learning models are linked to several issues that have been and can be solved by semi-supervised and unsupervised learning models introduced in the literature throughout the past few years. We conduct a detailed and comprehensive survey of various anomaly detection techniques that have been most widely used and have proven successful for detecting a range of financial fraud cases, with an emphasis on the recent developments in these fields pertaining to semi-supervised and unsupervised learning.

According to Zarka Zahoor and Karuna, (2016) in a research paper titled as "Challenges in Privacy and Security in Banking Sector and Related Countermeasures, 2016" the authors Killing of terrorism should march on the road lying on internet and easier access. Unfortunately, with this, cyber crimes related to banks are increasing tremendously. For example, the financial institutions industry has a wide variety of cyber-attacks, security, and information privacy, including Internet card processing, slip net banking transactions, and encryption. In the study which was conducted, it was concluded that these financial services were usually motivated by acquiring sensitive data or theft of funds from banks. These aren't ahows how they work either by the author, about how to swim better floating to help overcome problems.

Suling Feng Environment, decentralization, digital finance and green technology innovation Structural Change and Economic Dynamics, Volume 61, June 2022, Pages 70-83. Only through all traditional financial institutions actively adaptation to the digital trend, can improve the enterprise of green technology innovation ability and realize the solution of serious environmental pollution problem. Meanwhile, the government should formulate the differential innovation incentive policy to encourage manufacturing and individual enterprises to increase investment in scientific and technological innovation, and promote the reform of the environmental decentralization system and strengthen the supervision of the central environmental protection agency.

Digital twin for credit card fraud detection: opportunities, challenges and fraud detection advancements Pushpita Chatterjee, Future Generation Computer Systems Volume 158, 15 September 2024, Pages 410-426. The research (Pushpita Chatterjee, 20224) not only highlights the need for developing more sophisticated fraud detection mechanisms but also stresses the necessity of ongoing innovation and adaptation to improve financial security.

Credit card fraud detection in the era of disruptive technologies: A systematic review Journal of King Saud University – Computer and Information SciencesVolume 35, Issue 1, January 2023, Pages 145-174. Asma Cherif Credit card fraud is an increasingly severe and widespread issue triggered by the rise of new technologies and communication methods, such as contactless payment. Here, we provide a comprehensive review of the state-of-the-art research in detection and prediction of fraudulent credit card transactions, which was published between 2015 and 2021.

Dzomira, S. (2014), Electronic fraud (cyber fraud) risk in the banking industry Zimbabwe. Risk governance & control: financial markets & institutions, 4(2), 17-27. The paper discusses what types of electronic fraud are being perpetrated in the banking industry as well as what issues are being faced to mitigate risk. This paper make use of Descriptive study which studid Cyber Fraud phenomenon by using Content Analysis. For getting the data, 22 different banks were contacted to fill in the data questionnaires and conduct the interviews with the selected informants. Sampling technique were convenience and judgemental. (endpoint, 10) To a great extent, discipline gave way to proactive engagement addressing the lack of multiple purpose electronic fraud varieties across the banking industry. Corporate partners are increasingly aware of the importance

of growing cyber awareness within the corporate sector and also contributing to governmental awareness on laws and regulations through government contact, such skills development, training and knowledge sharing, and also conveying messages on political issues relating to lack of resources (detection tools and technologies) inadequate cyber-crime laws and lack of knowledge through education and awareness.

Soni R.R. and Soni Neena's (2023) article “An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks”, privately owned financial institutions do not adhere to basic security measures, while public sector banks keep performing conventional strategies. The article distinguishes between bank fraud inflation rates across both private and public financial institutions and runs into a suggestion that private institutions are more inclined to perpetrate fraud. The author has distinguished between public and private banks and the weight each bank carries in constituting cyber fraud but has failed to mention the measures and precautions which can be implemented by the banks in order to prevent the upsurge of Cyber crime.

Prasad & Meghwal (2017) the analysis of the study is digital financial literacy plays a crucial part in enhancing society's financial inclusion, and is the best weapon to face challenges. The research study comprised of households in Udaipur district of Rajasthan. Findings showed that people were concerned more about digital payments debit card, credit card, mobile banking etc. The males are found to be more digitally financial literate as compared to females. A context-sensitive education framework was proposed at the end of study.

Poh Xin Yi, Intan Farahama Binti Kamsin,et,al.,Implementation of One-Time Password in Online Banking System Among Malaysian Bank Users to Reduce Cyber Fraud International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429) (June 2023), 32-47. The goal of this approach is to enhance the novel features within the current system and the previously trivial aspect. Online banking applications has many issues once security is a main issue; it could be established through multiple of Internet technology. A study that can implemented on a lot of safe and effective ways to try and rid the user of the fear of being scammed by reducing the frequency of phishing attacks and verify the user’s identity. The critical weakness related to standard password-based systems has encouraged putting one-time password (OTP) systems into place for security.

He is vice chairperson at the Faculty of Prestige Institute of Management & Research, Indore and his research work is on Internet Users Resistance towards online Purchase an exploratory study. There are information-based platforms as well as transactional-based platforms. A large amount of people are not just using Internet to get their hands on the latest information, also using them to buy products online. This study would be useful for the marketers in strategising on online sales. The study also analyzes the efficacy of existing cyber security measures, such as multi-factor authentication and anti-phishing tools, and explores the challenges confronting law enforcement and regulatory authorities dealing with these offences.

In a study, we delve into the twofold nature of cyber fraud, focusing on both the technological and psychological components, to uncover successful approaches for combating the rise of cybercrime. One of the biggest global issues we are facing is cyber fraud and the same is with India as well. Two key dimensions encompass this phenomenon: the technological exploitation dimensions, and the psychological manipulation dimensions. Cybercriminals use sophisticated technology skillfully, but also psychological techniques that take advantage of people and can create huge financial losses. These criminals prey even further, targeting mainly people who are vulnerable, those who face mental health issues in particular because they will use these people anxiety, emotion, fear and depression against them. Cyber fraud affects people from all backgrounds educated and uneducated.

In a chronology of the financial sector in Indian history and the evolution with money lenders accumulating deposits and emitting receipts in their stead, the author paves the Indian Banking Sector: Then, Now, and the Road Ahead by Karishma Bhandari and Harvinder Soni (Vikrant Chopra, HarperCollins) The seizure of banks was an unprecedented shift in banking standards. Also, the merger of finance — and innovation — has been responsible for many the huge changes in the banking industry. The importance of technology innovation in enhancing productivity and making customer service more efficient. The author has covered all angles of innovation in tech, yet forgot to familiarize itself with the economic cons that shadowed all this innovation and progress.

In the book of Grabosky and Walkley (2007), titled as "International Handbook of Computer Crime and White Collar Crime", the researchers chronicled that digital and

white collar crimes were once conceived to be crimes without perpetrators, however with the tremendous quantities of money involved, such offences have grown to involve a considerable number of victims. Wide-ranging financial frauds have been extensively scrutinized, along with the variables that contribute to them. The researcher explains how the enforcement reacts to white-collar crime, as well as diverse conceptual strategies, legislative and regulatory views, and accessible judicial systems. The reduction and prevention of cyber and white-collar crime was considered by the researchers but they blurred out the very focus of the study that is to counter the issues of IMPS frauds and provide legal suggestions for the same.

In the book of Madharva Somo Sundaram and Umarhathab (2011), titled as "Cyber Crime and Digital Disorder", the researchers delineated that the law making bodies have been frequently proactive in combating Cyber fraud matters and thus they must be efficiently trained with the thorough and augmented knowledge of Cyber security in order to efficiently cope with such issues systematically. However, the study omitted any ideas for authority training.

3. RESEARCH OBJECTIVE

The objectives are as follows:

- The aim of this research project is to develop a more powerful technology to improve the online bank system. The research also identifies the security enhancements that would make an online bank system more security
- To examine how well India's legal system works to stop, identify, and prosecute online financial frauds.
- To understand the Cyber Security Techniques which can be used stop such malicious activities from rising.
- To analyse how courts are interpreting and applying cyber laws pertaining to digital financial crimes, review recent case legislation and court rulings.
- To identify areas for possible improvement, compare India's cyber laws with best practices from around the world.

4. RESEARCH METHODOLOGY

The methodology which the researcher adopted was mainly doctrinal. The current study is predominantly based on the doctrinal and analytical research. The thesis relies on primary as well as secondary data which was analysed to critically evaluated the problem and re-examine the present legislative framework in light existing facts and data collected.

The researchers primary analysed primary sources which include conventions, statues, laws, Reports by National Commission and International Organisations, case laws and treaties.

Secondary data has been extensively collected and referred including books, journals, articles, surveys, newspapers, magazines, and available interne sources. Additionally, other relevant sources were also employed wherever necessary to meaningfully examine the questions that this thesis strives to answer and inquire into. The footnotes and citations are followed in accordance with MRU guidelines.

5. HYPOTHESIS

1. The Challenges arising from digital financial frauds are not sufficiently addressed by current laws & regulations,
2. Victims of digital financial frauds face long delays in receiving redressal due to inefficiencies in existing legal process.
3. There are significant gaps in public awareness and digital literacy, which contribute to the rising cases of digital frauds in India.

6. RESEARCH QUESTIONS

1. Whether current cyber laws in India prove effective in deterring and prosecuting incidents of digital financial fraud?
2. Whether the financial institutions and digital platforms in India adhere to cyber laws concerning digital financial fraud?
3. Whether the ongoing cybersecurity education and awareness efforts proving successful in mitigating digital fraud in India?
4. Whether financial institutions and digital payment systems handle the risk of fraud, and what can be done better?
5. Whether technology like block chain and machine learning be used to identify and stop online financial frauds?

7. Tentative Chapterisation

Chapter 1: Introduction

Chapter 2: Digital Financial Frauds: A Conceptual Framework

Chapter 3: International Framework

Chapter 4: An Overview of Legal & Regulatory framework in India

Chapter 5: Comparative analysis and best practices

Chapter 6: Role of banks & Financial Institutions, FinTech, forensics and AI in combating Digital Cyber Frauds

Chapter 7: Conclusion and Suggestions

8. Bibliography:

1. Kumar, Vijay. "Digital Hotspots." In *The Economic Value of Digital Disruption: A Holistic Assessment for CXOs*, pp. 689-795. Singapore: Springer Nature Singapore, 2023.
2. Beju, Daniela-Georgeta, and Codruța-Maria Făt. "Frauds in Banking System: Frauds with Cards and Their Associated Services." In *Economic and Financial Crime, Sustainability and Good Governance*, pp. 31-52. Cham: Springer International Publishing, 2023.
3. Jaiswal, Kajal. "Effectiveness of cybercrime laws and regulations in India: A critical study." (2022).
4. The Information Technology Act, 2000
5. Kashyap, Amit Kumar, and Mahima Chaudhary. "Cyber security laws and safety in e-commerce in India." *Law & Safety*, 207 (2023).
6. Qian, Xu. "Redefining International Law Paradigms: Charting Cybersecurity, Trade, and Investment Trajectories within Global Legal Boundaries." *The Journal of World Investment & Trade* 25, no. 3, 295-333 (2024).
7. Kumar, Chaman. "Legal Perspective on Cryptocurrency Regulation-Regulatory Framework and Challenges." *Jus Corpus LJ* 4, 1 (2023).
8. Khurana, Rahul. "Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management." *International Journal of Applied Machine Learning and Computational Intelligence* 10, no. 6, 1-32 (2020).
9. Juneja, Ashish, Shankha Shubhra Goswami, and Surajit Mondal. "Cyber security and digital economy: opportunities, growth and challenges." *Journal of technology innovations and energy* 3, no. 2, 1-22 (2024).
10. Fouillet, Cyril, Isabelle Guérin, and Jean-Michel Servet. "Demonetization and digitalization: The Indian government's hidden agenda." *Telecommunications Policy* 45, no. 2, 102079 (2021).
11. Ratnoo, Preeti. "Navigating the crossroads: Crypto assets in India-Secutity, currency or an uncharted territory." PhD diss., National Law School Of India University, 2024.

12. EFG, Ajayi. "The Challenges to Enforcement of Cybercrimes Laws and Policy." *International Journal of Information Security & Cybercrime* 4, no. 2 (2015).
13. Ajayi, Emmanuel Femi Gbenga. "Challenges to enforcement of cyber-crimes laws and policy." *Journal of Internet and Information Systems* 6, no. 1, 1-22 (2016).
14. Saluja, Shefali. "Identity theft fraud-major loophole for FinTech industry in India." *Journal of Financial Crime* 31, no. 1, 146-157 (2024).
15. Collier, Ben, Daniel R. Thomas, Richard Clayton, Alice Hutchings, and Yi Ting Chua. "Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services." *Policing and Society* 32, no. 1, 103-124 (2022).
16. 2024 SCC online bom 1666.
17. W.P. No. 28421 of 2022.
18. **AIR 2015 SUPREME COURT** 1523, 2015
19. Gayathri, S. "A critical analysis of the punjab national bank scam and its implications." *International Journal of Pure and Applied Mathematics* 119, no. 12, 14853-14866. (2018).
20. Sharma, Abhishek. "Cyber Crimes and India's National Security: A Rising Threat in the Cyber Domain." *Defence & Diplomacy* 13, no. 2, 87-99 (2024).
21. Sun, Guanglin, Ting Li, Yongfang Ai, and Qinghai Li. "Digital finance and corporate financial fraud." *International Review of Financial Analysis* 87, 102566 (2023).
22. Brent Clyton Harker, "Criminal Law" 5 *Issues in Information Systems Volume* 35-48 (2023).
23. Broadstock, David, and Xiaoqi Chen. "Corporate site visits, private monitoring and fraud: Evidence from China." *Finance Research Letters* 40, 101780 (2021).
24. Hilal, Waleed, S. Andrew Gadsden, and John Yawney. "Financial fraud: a review of anomaly detection techniques and recent advances." *Expert systems With applications* 193 (2022): 116429.
25. Zahoor, Zarka, Moin Ud-din, and Karuna Sunami. "Challenges in privacy and security in banking sector and related countermeasures." *International Journal of Computer Applications* 144, no. 3, 24-35 (2016).

26. Feng, Suling, Rong Zhang, and Guoxiang Li. "Environmental decentralization, digital finance and green technology innovation." *Structural Change and Economic Dynamics* 61, 70-83 (2022).
27. Chatterjee, Pushpita, Debashis Das, and Danda B. Rawat. "Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements." *Future Generation Computer Systems* (2024).
28. Cherif, Asma, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, and Abdessamad Imine. "Credit card fraud detection in the era of disruptive technologies: A systematic review." *Journal of King Saud University-Computer and Information Sciences* 35, no. 1, 145-174 (2023).
29. Dzomira, Shewangu. "Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe." *Risk Governance and Control: Financial Markets and Institutions* 4, no. 2, 16-24 (2014).
30. Soni, R. R., and Soni Neena. "An investigative Study of Banking cyber frauds with special reference to private and public sector banks." Research Journal of Management Sciences ISSN 2319, 1171 (2013).
31. Sen, Dishani. "How age impacts participation in digital economy in India: A narrative research approach." 43-56 (2020).
32. Yi, Poh Xin, Intan Farahana Kasmin, Salmiah Amin, and Nur Khairunnisha Zainal. "Implementation of One-Time Password in Online Banking System Among Malaysian Bank Users to Reduce Cyber Fraud." *International Journal of Data Science and Advanced Analytics* 4, 20-26 (2022).
33. Balabantaray, Subhra Rajat. "Examining the Impact of Cyber Fraud on Indian Society: An Assessment of the Potential Damage." In *Cybersecurity, Law, and Economics*, pp. 38-50. Routledge, 2024.
34. Bhandari, Karishma, and Harvinder Soni. "Indian Banking Sector: Then, Now & the Road Ahead." *International Research Journal of Engineering and Technology (IRJET)* 3, no. 4 (2016).
35. Grabosky, Peter, and Sascha Walkley. "Computer crime and white-collar crime." In *International handbook of white-collar and corporate crime*, pp. 358-375. Boston, MA: Springer US, 2007.
36. Sundaram, P. Madhava Soma, and Syed Umarhathab, eds. *Cyber crime and digital disorder*. Publication Division, Manonmaniam Sundaranar University, 2011.

MANAV RACHNA UNIVERSITY

Swami Vivekananda Library and Resource Centre
Manav Rachna University

SIMILARITY VERIFICATION CERTIFICATE

Title: A Digital Financial Frauds : A Critical Analysis of Cyber Laws in India

Researcher: MANISHA AHLAWAT

Registration Number: [illegible]

Supervisor: Dr. Aditi Chaudhary

Department: School of Law

This is to certify that the above mentioned Short Synopsis/Thesis was scanned for similarity index through Drill Bit Software on 2 March 25 with submission ID 3.440670 and the similarity index was found to be 4 %. The complete report running into 17 Pages 9.7.70 Word count with File Size 13.47 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

Date: 2 April 2025

The complete report of the above Short Synopsis/Thesis has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/Thesis may be considered for further processing

Research Scholar

2/4/25

Research Supervisor

DrillBit

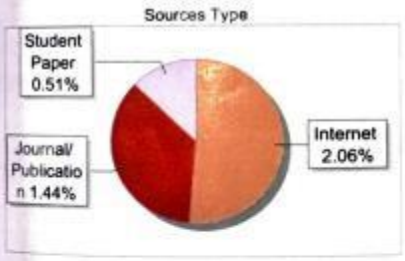
The Report is Generated by DrillBit Plagiarism Detection Software

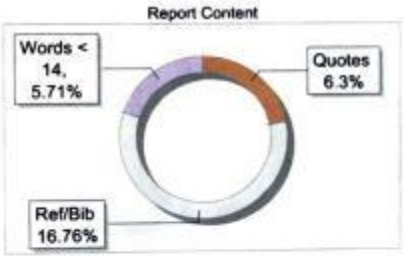
Submission Information

Author Name	Manisha Ambawta
Title	DIGITAL FINANCIAL FRAUDS: A CRITICAL ANALYSIS OF THE CYBER LAWS IN INDIA
Paper Submission ID	3440670
Submitted by	netrapal.library@mru.edu.in
Submission Date	2025-03-27 15:06:23
Total Pages, Total Words	17, 4940
Document type	Synopsis

Result Information

Similarity 4 %





Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Source: Excluded < 14 Words	Excluded
Excluded Source	0 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

Excluding matches
less than 14 words

DrillBit

DrillBit Similarity Report

A-Satisfactory (0-10%)
B-Upgrade (11-40%)
C-Poor (41-60%)
D-Unacceptable (61-100%)

4	8	A
SIMILARITY %	MATCHED SOURCES	GRADE

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
3	fastercapital.com	1	Internet Data
4	crl.acrl.org	1	Publication
5	www.sciencedirect.com	1	Internet Data
6	Acharyanagarjuna University Thesis Published in Shodganga www.infilibnet.ac.in	1	Student Paper
7	eajournals.org	<1	Publication
8	mnit.ac.in	<1	Internet Data
9	www.iarj.in	<1	Publication
10	www.academia.edu	<1	Internet Data

DIGITAL FINANCIAL FRAUDS: A CRITICAL ANALYSIS OF THE CYBER LAWS IN INDIA

SHORT SYNOPSIS

By

Manisha Ambawta
Registration No.
MRULWDM012K230066

Under the supervision of

Name of Supervisor
Dr. Aditi Chaudhary

Year *2023-24*

ABSTRACT

With most transactions going digital in India at such a rapid pace, there is a rise in digital financial frauds posing a great challenge for individuals and businesses and financial institutions as well. Even though the Indian government has introduced several cyber laws, including the Information Technology Act, 2000, and regulatory frameworks by the Reserve Bank of India, the increasing sophistication of cybercriminals continues to expose gaps in the current legal and enforcement frameworks. In this study, we critically evaluate the Indian cyber laws related to digital financial fraud, identify the legal vacuum and recommend measures to strengthen the cyber security architecture. Research Objectives: To devise innovative technologic solutions for security enhancement of online banking system To analyze efficacy of

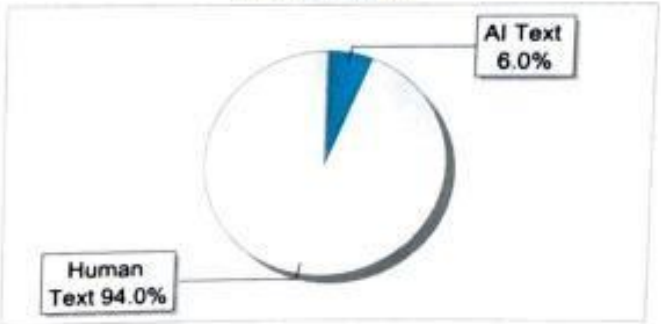
DrillBit

The Report is Generated by DrillBit AI Content Detection Software

Submission Information

Author Name	Manisha Ambawta
Title	DIGITAL FINANCIAL FRAUDS: A CRITICAL ANALYSIS O
Paper/Submission ID	3440670
Submitted By	netrapal.library@mru.edu.in
Submission Date	2025-03-27 15:06:23
Total Pages	17
Document type	Synopsis

Result Information

AI Text: 6 %

Content Matched